УДК 004.4:519.713

Обеспечение информационной защиты беспроводных сенсорных сетей на основе клеточных автоматов

© Ив.И. Захарчук[1], Ил.И. Захарчук[1], Ю.Г. Веселов[2], А.С. Островский[2]

[1] Военно-космическая академия им. А.Ф. Можайского, Санкт-Петербург, 197198, Россия
[2] МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Необходимость автоматизированного сбора больших объемов информации об окружающей обстановке требует поиска новых, более совершенных технических средств. Беспроводные сенсорные сети могут являться одним из способов контроля измеряемых физических параметров на обширных территориях. Такие децентрализованные самоорганизующиеся сети из миниатюрных автономных узлов-сенсоров могут осуществлять сбор, накопление и передачу путем ретрансляции от узла к узлу информации в единую точку сбора, при этом не нуждаясь в предустановленной опорной сетевой инфраструктуре. Однако низкая производительность элементов беспроводной сенсорной сети, обусловленная энергетическими и массогабаритными ограничениями, а также децентрализованный характер сети делает традиционные методы обеспечения информационной безопасности неприменимыми. Одним из путей преодоления накладываемых ограничений является распараллеливание алгоритмов криптозащиты. В данной статье рассмотрен подход к организации процесса криптографических преобразований на основе клеточных автоматов. Предложены различные методы применения аппарата клеточных автоматов для решения задач криптографической защиты информации.

Ключевые слова: *беспроводные сенсорные сети, информационная безопасность, криптографическая защита данных, гомогенные структуры, клеточные автоматы.*

Введение. Непрерывное развитие вычислительных средств и сетевых технологий постоянно оказывает влияние на развитие способов вооруженного противоборства. Происходит непрекращающееся проникновение геоинформационных систем, автоматизированных систем управления, различных интеллектуальных и экспертных систем поддержки принятия решений в процесс управления войсками. Работа таких систем требует эффективного выполнения функций автоматизированного сбора, накопления и обработки разнородной информации о состоянии окружающей обстановки. С увеличением объема поступающей информации, ужесточением требований к ее полноте и оперативности сбора в целях увеличения скорости и качества управления возникает необходимость поиска новых средств ее сбора.

Решением данной проблемы могут стать беспроводные сенсорные сети (wireless sensor networks — WSN). Беспроводная сенсорная сеть представляет собой пространственно распределенную самоорганизующуюся систему автономных миниатюрных датчиков (сенсоров или узлов), способных измерять определенные физические параметры окружающей среды, а затем совместно передавать накопленную информацию, ретранслируя ее от узла к узлу через образованную самими датчиками беспроводную сеть в единую точку сбора. Такие сенсорные сети позволяют контролировать измеряемые параметры окружающей среды на значительных пространствах, а также считывать показания всей сети, подключившись к ее произвольному узлу.

Гибкая архитектура, снижение затрат при развертывании выделяют беспроводные сенсорные сети среди других систем сбора информации, особенно когда речь идет о большом количестве соединенных между собой устройств. Например, разрабатываемая агентством DARPA система Smart Dust состоит из миниатюрных сенсорных узлов (размеры каждого узла составляют несколько кубических миллиметров), которые могут разбрасываться на значительных площадях, в том числе с помощью авиации, и затем самоорганизовываться в единую сенсорную сеть. При этом сеть должна быть устойчива к выходу из строя части узлов. Кроме того, она должна быть способна восполнять потери и расширяться за счет расположения впоследствии новых сенсорных узлов.

В связи с невозможностью ограничить доступ к физической среде беспроводной связи, а также из-за децентрализованного характера сенсорных сетей проблема обеспечения в них информационной безопасности стоит особенно остро. Информационный обмен в недоверенной сетевой среде вынуждает к широкому использованию криптографических средств защиты информации. Ограниченные вычислительные и энергетические ресурсы сенсорных узлов [1], с одной стороны, и потребность в непрерывном шифровании регистрируемой и передаваемой сенсорами информации — с другой, требуют поиска новых криптографических методов защиты передаваемой информации.

Постановка задачи. В основе существующих криптосистем лежат последовательные вычислительные алгоритмы. Применение технологий распараллеливания таких алгоритмов не позволяет значительно повысить эффективность процесса генерации последовательностей с позиций затрат и производительности, так как рост потребностей опережает линейный рост возможностей кремниевых технологий. Усилия исследователей все более сосредоточиваются на поиске новых вычислительных моделей, реализующих изначально

параллельные способы решения триединой задачи: криптозащиты, имитозащиты и защиты данных от случайных сбоев при преобразовании и передаче.

В качестве такой вычислительной модели может выступать клеточный автомат (КЛА) — бесконечная сеть одинаковых автоматов Мура, расположенных в точках пространства с целочисленными координатами, связанных одинаковым образом друг с другом и изменяющих состояние в зависимости от состояний соседей и своего собственного. Динамика состояний однородной пространственно распределенной дискретной системы с локальным взаимодействием элементов может представлять разнообразные варианты поведения (устойчивые конфигурации, циклы, хаос), в том числе не имеющие прямого аналога среди аттракторов непрерывных динамических систем. Такая система в силу однородности и локальности преобразований устойчива к сбоям отдельных элементов.

Алгоритмическая неразрешимость прямой задачи — синтеза функции глобальных (для всех элементарных автоматов) переходов КЛА по локальной функции и обратной задачи — определения структуры и параметров КЛА по множеству его состояний позволяет использовать такую модель в качестве криптосистемы.

Криптосистемы на клеточных автоматах могут быть как симметричными, так и асимметричными. В случае симметричных криптосистем ключом может служить, например, начальное состояние клеточного автомата, осуществляющего генерацию псевдослучайной последовательности состояний и преобразование открытого текста на основе только локальных правил перехода. Для реализации асимметричных криптосистем могут использоваться обратимые клеточные автоматы [2]. В этом случае в качестве открытого ключа может выступать, например, локальная функция переходов. Для двумерных КЛА отыскание функции, инверсной к заданной локальной функции переходов, относится к числу алгоритмически неразрешимых задач [1]. Поэтому важным направлением исследования является поиск универсальных обратимых КЛА.

Проблему универсальности КЛА можно рассматривать в двух аспектах. В рамках первого универсальность сводится к представлению одних КЛА в других. Клеточный автомат является универсальным, если он моделирует поведение любого другого КЛА той же размерности.

Другой подход к универсальности восходит к универсальной вычислимости. Клеточный автомат является универсальным, если он моделирует универсальную машину Тьюринга. Представляет интерес поиск КЛА с минимальными значениями параметров. Следует отме-

тить, что в общем виде проблема распознавания представимости КЛА также относится к числу алгоритмически неразрешимых.

Модель. Формализуем задачу в терминах теории клеточных автоматов.

Клеточный автомат K есть упорядоченное множество из четырех компонент

$$K = \left\langle Z^d, N, Q, \varphi \right\rangle, \tag{1}$$

где Z^d — множество d-мерных векторов с целочисленными координатами — клеточное пространство (рис. 1);

$N = \left\{ n_i \middle| n_i = \left(x_{1i}, ..., x_{di} \right), \exists n_i = 0 \right\}$, $i = 1, ..., m$, — конечное множество мощности m векторов из Z^d с нулевым вектором — шаблон соседства КЛА;

Q — конечное множество мощности k состояний клетки с выделенным состоянием покоя $\varnothing$ — алфавит клеточного автомата;

$\varphi\colon Q^m \to Q$ — локальная функция переходов, определенная на множестве элементов окрестности в дискретные моменты времени $\varphi\left(\varnothing_0, \varnothing_1, ..., \varnothing_{m-1} \right) = \varnothing$.

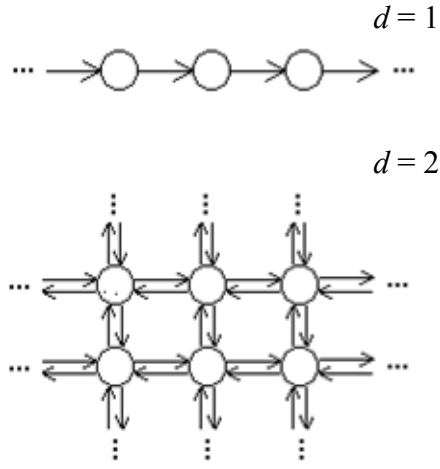

Рис. 1. Варианты клеточного пространства

Состояние всех клеток на момент времени t образует текущую конфигурацию $c_t\colon Z^d \to Q$. Применение локальной функции переходов к текущей конфигурации задает глобальную функцию переходов $c_{j+1} = f\left(c_j \right)$.

Упорядоченная совокупность конфигураций, получаемая из начальной последовательным применением глобальной функции переходов, образует эволюцию e клеточного автомата $e = < c_0, c_1, ..., c_\tau >$. В общем случае $\text{card}\, e = \aleph_0$.

Одномерные клеточные автоматы, у которых $m = 2$ или $k = 2$, будем называть *ординарными*. Шаблон, у которого по каждой координате имеется единственный сосед, находящийся на единичном расстоянии от центрального, будем называть *Z-шаблоном*, а шаблон, образующий *d*-мерный единичный куб, — *S-шаблоном*. Для двумерного КЛА (рис. 2) *Z*-шаблон — $(d = 2, m = 3)$, *S*-шаблон — $(d = 2, m = 4)$, *N*-шаблон Неймана — $(d = 2, m = 5)$, *M*-шаблон Мура — $(d = 2, m = 9)$. Кроме числа элементов m шаблоны двумерных КЛА будем характеризовать сторонами прямоугольника, описывающего данный шаблон, — x и y.

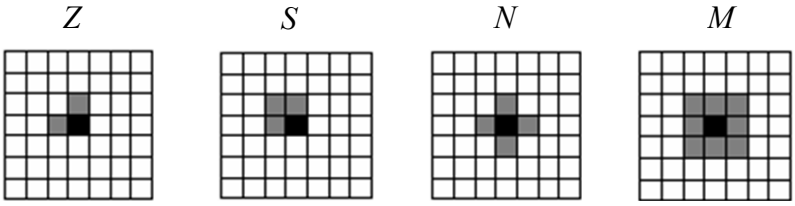

Рис. 2. Варианты шаблонов для двумерного КЛА

По аналогии с введенной Шенноном сложностью универсальных машин Тьюринга произведение $C_s = d \times m \times k$ задает сложность универсальных КЛА.

Клеточный автомат K^* моделирует поведение клеточного автомата K с замедлением *n*, если для любой эволюции $e \in E$, допускаемой клеточным автоматом *K*, существует гомоморфизм $h: E \to E^*$, причем $c_j = h\left(c^*_{nj}\right)$. При $n = 1$ будем говорить, что моделирование осуществляется в реальном времени.

Решения. 1. ***Инварианты.*** Первым значимым классом, для которого были получены продвижения в задаче распознавания свойства обратимости, стал класс одномерных КЛА. В [3] было установлено, что в этом классе существует алгоритм для распознавания обратимости. В той же работе высказана гипотеза, что для многомерных КЛА свойство обратимости также разрешимо, и даже было предложено попытаться обобщить на них технику одномерного случая. Однако в работе [4] было установлено, что задача распознавания свойства об-

ратимости для КЛА размерности 2 и более ($d \geq 2$) является алгоритмически неразрешимой.

Следующий вопрос, связанный с обратимыми КЛА, — это вопрос о доле их в множестве всех клеточных автоматов. С помощью усиления теоремы Мура – Майхилла можно показать, что почти все клеточные автоматы являются необратимыми. В настоящее время в литературе класс обратимых КЛА часто упоминался как класс малой мощности (таблица).

Пример параметров обратимых одномерных КЛА

$\|Q\|$	$\|N\|$	Общее число функций		Число эквивалентных классов
		локальных	обратимых	
2	2	16	4	1
	3	256	6	1
	4	65 536	16	2
	5	$4{,}3 \cdot 10^9$	62	7
3	2	19 638	48	3
	3	$7{,}6 \cdot 10^{12}$	1776	101
4	2	$4{,}3 \cdot 10^9$	5184	≈ 60

В [5] было установлено, что асимптотика логарифма числа обратимых клеточных автоматов в любом классе КЛА с фиксированным шаблоном соседства совпадает с асимптотикой числа всех клеточных автоматов.

Важным вопросом в исследовании свойства обратимости является поиск топологических параметров универсальных КЛА, позволяющих моделировать произвольные клеточные автоматы. При этом в [6] были сформулированы и доказаны следующие **теоремы**:

1. Любой одномерный КЛА K с шаблоном соседства m моделируется с замедлением, равным $m-1$, ординарным КЛА K_{o} с числом состояний $k_{\text{o}} \leq \sum_{i=1}^{m} k^i$.

2. Любой одномерный КЛА K моделируется в реальном масштабе времени ординарным КЛА K_{o} с шаблоном соседства

$$m_{\text{o}} \leq \left(m \left| \log_2 2k^2 \right| - 2 \right).$$

3. Существует универсальный ординарный КЛА K_{o}^{u} со сложностью $C_s = 1 \times 16 \times 2$.

4. Клеточный автомат с *Z*-шаблоном K_Z моделирует поведение любых двумерных клеточных автоматов с шаблоном Неймана K_N с

трехкратным замедлением, при этом число состояний возрастает до $k_Z = k_N^3 + k_N^2 + k_N$.

5. Клеточный автомат с *Z*-шаблоном K_Z моделирует поведение любых двумерных клеточных автоматов с шаблоном Мура K_M с четырехкратным замедлением, при этом число состояний возрастает до $k_Z = k_M^4 + k_M^3 + k_M^2 + k_M$.

6. Клеточный автомат с *Z*-шаблоном K_Z моделирует поведение любых двумерных клеточных автоматов K с замедлением n, при этом $k_Z \le \sum_{i=1}^{n} k^i$, $n = x + y - 2$.

Увеличение числа соседей на единицу (*S*-шаблон) приводит к следующим результатам.

7. Клеточный автомат с *S*-шаблоном K_S моделирует поведение двумерных клеточных автоматов *K*, имеющих шаблоны Мура или Неймана, с двухкратным замедлением, при этом $k_S = k^4 + k$.

8. Клеточный автомат с *S*-шаблоном K_S моделирует поведение любых двумерных клеточных автоматов K с замедлением n, при этом $k_S \le \sum_{i=1}^{n} k^{i^2}$, $n = \max(x, y) - 1$.

2. *Обобщенная модель.* В определении КЛА может быть расширена как область допустимых топологических структур, так и область локальных функций. Так, структуры, приведенные на рис. 3, не попадают в область допустимых структур определения (1), хотя представлены однородными графами.

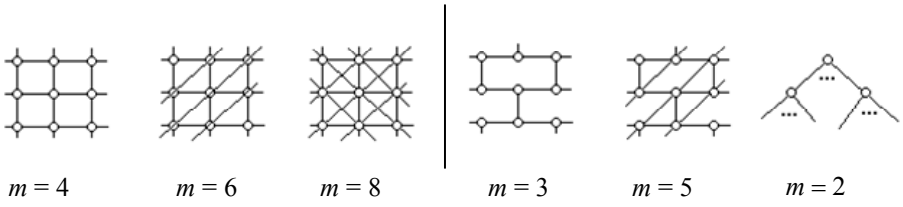

Рис. 3. Типы топологических структур (справа), не представленных классическими КЛА (слева)

Аналогично графы, являющиеся группами движений нескольких многоугольников, не описываются выражением (1). Однако эти структуры могут быть сведены к решеткам, определенным в классических КЛА (пример представлен на рис. 4), и, следовательно, отнесены к классу КЛА.

Предлагается обобщенная модель клеточного автомата — кортеж

$$K = \langle G_R^d(V), \Phi \rangle, \qquad (2)$$

где $G_R^d(V)$ — топологическая структура КЛА — бесконечный граф с множеством вершин V группы движений фундаментальной области R в пространстве размерности d (регулярный граф); $\Phi = \{\varphi_1, \varphi_2, ..., \varphi_r\}$ — локальный оператор переходов ($\varphi_i : Q^m \to Q$ — локальная функция переходов i-й вершины фундаментальной области; Q — множество состояний каждой клетки, $|Q| = k$, $\varnothing \in Q$, $\varphi(\varnothing_0, \varnothing_1, ..., \varnothing_{m-1}) = \varnothing$; $m = \deg^-(v_i) + 1$, $v_i \in V$, — полустепень захода i-й вершины фундаментальной области).

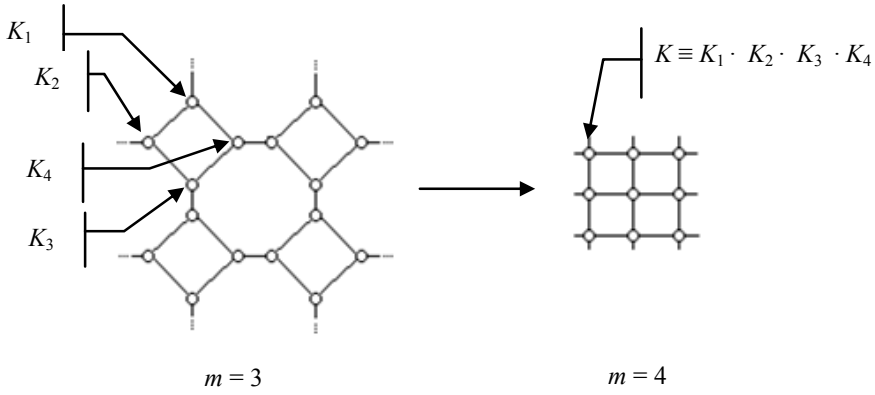

Рис. 4. Неоднородные автоматные сети, преобразуемые к классическим КЛА

Обобщенная модель (2) расширяет как множество возможных топологических структур, так и множество локальных функций переходов. Она позволяет использовать регулярные графы, сводящиеся к однородным, и композицию локальных функций.

3. ***Алгебра клеточных автоматов.*** Для объединения «элементарных» клеточных автоматов в функционально более сложные вводятся операции над КЛА: n-арные операции параллельного и последовательного соединения КЛА, склейки и расслоения КЛА, унарная операция взятия проекции. Данный «инструментарий» позволяет выделить три подхода к обеспечению функционирования в условиях сбоев элементов. Первый связан с увеличением числа соседних элементов. В основе второго лежат идеи корректирующего кодирования состояний элементов-клеток. Третий метод является комбинированным и связан с использованием инвариантов при взаимном моделировании клеточных автоматов. Таким образом, возможны следующие операции над КЛА:

1. *Объединение (параллельное соединение) клеточных автоматов* $K \equiv K_1 \otimes K_2 \otimes ... \otimes K_l$. Объединением клеточных автоматов будем называть клеточный автомат, алфавит состояний которого и множество эволюций являются декартовым произведением состояний и эволюций объединяемых клеточных автоматов: $E \equiv E_1 \times E_2 \times ... \times E_l$, $Q \equiv Q_1 \times Q_2 \times ... \times Q_l$. Операция обладает свойством коммутативности и ассоциативности: $K_1 \otimes (K_2 \otimes K_3) = (K_1 \otimes K_2) \otimes K_3$, $K_1 \otimes K_2 = K_2 \otimes K_1$.

2. *Композиция (последовательное соединение) клеточных автоматов* $K \equiv (...(K_1 \oplus K_2) \oplus ...) \oplus K_l$. При последовательном соединении заключительная конфигурация одного автомата является начальной другого: $\forall e \in E \quad e = \langle c_{01}, ..., c_{\tau 1}, c_{12}, ..., c_{\tau 2}, ..., c_{\tau l} \rangle$, $K = K_1 \oplus K_2 \oplus ... \oplus K_l$. Данная операция не обладает свойством коммутативности и ассоциативности $K_1 \oplus (K_2 \oplus K_3) \neq (K_1 \oplus K_2) \oplus K_3$, $K_1 \oplus K_2 \neq K_2 \oplus K_1$.

3. *Взятие проекции клеточного автомата* $K \equiv K^{(i)}$. Существо этой унарной операции определяется выражением $c_\tau(K) = c_i(K)$.

4. *Склейка клеточных автоматов* $K \equiv K_1 \cdot K_2 \cdot ... \cdot K_l$. Для данной операции $Q = Q_1 \times Q_2 \times ... \times Q_l$, $\varphi = f(\varphi_1, \varphi_2, ..., \varphi_l)$. Операция коммутативна и ассоциативна. Геометрическая интерпретация склейки представлена на рис. 4.

5. *Расслоение клеточного автомата* $K \equiv K_1 \circ K_2 \circ ... \circ K_l$. Эта операция является обратной операции склейки.

В работе [7] исследуются свойства генератора псевдослучайных последовательностей на базе одномерного КЛА с бинарным алфавитом, реализующего локальную функцию вида

$$q_i^{t+1} = q_{i-1}^t \oplus \left(q_i^t \vee q_{i+1}^t \right).$$

Конфигурации такого КЛА образуют последовательность двоичных случайных векторов.

Используя операции предложенной алгебры, можно получать другие КЛА, генерирующие псевдослучайные векторы. Так, в результате операции склейки двух КЛА, элементарные автоматы которых реализуют линейные преобразования над бинарным алфавитом

$$q_i^{t+1} = q_{i-1}^t \oplus q_{i+1}^t,$$

$$q_i^{t+1} = q_{i-1}^t \oplus q_i^t \oplus q_{i+1}^t,$$

получают генератор псевдослучайных последовательностей, изоморфный генераторам последовательностей на регистрах сдвига с линейными обратными связями.

Заключение. Анализ приведенных результатов показывает, что они дают на порядок менее сложные клеточные автоматы по сравнению с представленными в [7]. При этом линейный рост скорости работы за счет увеличения числа соседей сопровождается полиномиальным ростом числа состояний. Отметим, что увеличение числа состояний для моделирования произвольных двумерных КЛА простейшими КЛА совпадает с аналогичными результатами для простейших одномерных автоматов [6].

ЛИТЕРАТУРА

[1] Jurdak R. *Wireless Ad Hoc and Sensor Networks: A Cross-Layer Design Perspective.* Springer, 2007, p. 59.

[2] Захарчук И.И. Криптосистемы на клеточных автоматах. *Материалы II Межрег. конф. «Информационная безопасность регионов России» (ИБРР-2001)*. Санкт-Петербург, 26–29 ноября 2001 г. Санкт-Петербург, 2001, т. 1, с. 100.

[3] Amoroso S., Patt Y.N. Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures. *J. Computer and System Sci*, 1972, vol. 6, no. 5, pp. 448–464.

[4] Kari J. Reversibility of 2d cellular automata is undecidabale. *Physica D*, 1990, no. 45, pp. 149–182.

[5] Кучеренко И.В. О числе обратимых однородных структур. *Дискретная математика*, 2003, т. 15, № 2, с. 123–127.

[6] Захарчук И.И. О сложности одномерных универсальных клеточных автоматов. *Дискретный анализ и исследование операций,* 2002, сер. 1, т. 9, № 4, с. 50–56.

[7] Smith III A.R. Cellular automata complexity trade-offs. *Information and control*, 1971, vol. 18, pp. 466–482.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Захарчук Ив.И., Захарчук Ил.И., Веселов Ю.Г., Островский А.С. Обеспечение информационной защиты беспроводных сенсорных сетей на основе клеточных автоматов. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1003.html

Захарчук Иван Илларионович родился в 1986 г., окончил Военно-космическую академию им. А.Ф. Можайского в 2008 г. Адъюнкт Военно-космической академии им. А.Ф. Можайского. Автор 10 научных работ. Область научных интересов: децентрализованные самоорганизующиеся системы, информационная безопасность в сетевых распределенных структурах. e-mail: vzx313@gmail.com

Захарчук Илларион Иванович родился в 1958 г., окончил Военно-космическую академию им. А.Ф. Можайского в 1980 г. Канд. техн. наук, профессор кафедры Военно-космической академии им. А.Ф. Можайского. Автор более 60 научных и учебно-методических трудов. Область научных интересов: организация вычислений в сложных распределенных структурах, клеточные автоматы.

Веселов Юрий Геннадьевич родился в 1977 г., окончил Воронежский военный авиационный инженерный институт в 1999 г., адъюнктуру ВВИА им. проф. Н.Е. Жуковского в 2004 г. Канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор более 100 научных и учебно-методических трудов (учебника и 4 учебных пособий) в области интеллектуальных систем информационной безопасности, распознавания образов и оценки технического состояния систем получения видовой информации. e-mail: vesel_foto@mail.ru

Островский Александр Сергеевич родился в 1988 г., окончил Военно-воздушную академию им. проф. Н.Е. Жуковского и Ю.А. Гагарина в 2011 г. Канд. техн. наук, ассистент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор более 50 научных трудов в области информационной безопасности, оценивания защищенности сложных систем и оценки эффективности систем получения видовой информации.